REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1. Restriction Requirement

The Applicant notes the Examiner's argument that it is proper under the unity rules to arbitrarily restrict, at the Examiner's "discretion," claims that have already been twice examined. In reply, the Applicant invites the Examiner to consider MPEP §1850, part IV, which states that:

> *If little or no additional search effort is required, reasons of economy may make it advisable for the examiner, while making the search for the main invention, to search at the same time, despite the non-payment of additional fees, one or mote additional inventions in the classification units consulted for the main invention. The international search for such additional inventions will then have to be completed in any further classification units which may be relevant, when the additional search fees have been paid. This situation may occur when the lack of unity of invention is found either "a priori" or "a posteriori."*

Surely, when the search for all inventions has already been carried out, then reasons of economy would make it advisable to examine all of the claims, even if the Examiner also requires additional search fees per unity of invention practice.

Furthermore, the Applicant wishes to note that under the unity rules (see MPEP §1850, part III (A) and/or (B), and MPEP 1893(d) (explaining that "specially adapted" does not require that the product be exclusively for use with the process)), **restriction between an apparatus** (the data carrier of claims 1-21) **and a method of use** (the method of claims 26-33 and 42) **is *improper*.** Therefore, withdrawal of the requirement at least with respect to claims 1021, and examination of claims 1-21 on the merits without additional fees, is respectfully requested.

2. Rejection of Claim 42 Under 35 USC §112, 2nd Paragraph

This rejection has been addressed by amending claim 42 to delete "security-relevant," thereby correcting the antecedence error.

3. Rejection of Claims 26-32 and 42 Under 35 USC §102(e), and Rejection of Claim 33 Under 35 USC §103(a), in view of U.S. Patent No. 6,049,613 (Jakobsson)

This rejection is respectfully traversed on the grounds that the Jakobsson patent does not disclose or suggest the steps of:

- falsifying the input data by combination with auxiliary data (*Z*) before execution of one or more operations (*f*),
- combining the output data determined by execution of the one or more operations (*f*) with an auxiliary function value (*f*(*Z*)) in order to compensate for the falsification of the input data,
- wherein the auxiliary function value (*f*(*Z*)) was previously determined by execution of the one or more operations (*f*) with the auxiliary data (*Z*) as input data in safe surroundings and stored along with the auxiliary data (*Z*),

as recited in claims 26-32 and 42.

The Examiner is correct that claim 26 does not recite operation falsification in addition to input data falsification. However, the Jakobsson patent still does not teach the claimed invention since it does not teach an "auxiliary function value (*f*(*Z*))" that "was previously determined by execution of the one or more operations (*f*) with the auxiliary data (*Z*) as input data in safe surroundings and stored along with the auxiliary data (*Z*), as recited in claim 26. In particular, Jakobsson does not teach that the result of applying the function f to the auxiliary data Z is used to compensate for combination of the original input data with the auxiliary data.

While the "blinding" steps of Jakobsson could be considered to "falsify" input data by combination with auxiliary data, Jakobsson does not attempt to calculate the claimed auxiliary function such that f(Z) compensates for f(input data combined with Z) in order to recreate f(input data). Jakobsson has no need to do so because Jakobsson's re-encryption is used solely to compare the operations of parallel processors and determine whether the processors are functioning correctly or cheating. In fact, the outcome of Jakobsson's combination of processors is not f(input data combined with Z), *i.e.*, an operation on falsified input data, but rather the original input data that has been "permuted" (the order of the original data has been changed).

The reason why Jakobsson does not attempt to falsify input data and then obtain the same result as if the input data had not been falsified is that, in the method of Jakobsson, the data itself, which consists of **election results**, is <u>not secret</u>. In fact, it <u>must</u> not be changed. The only secret is who voted for whom, *i.e.*, the order of results. <u>The purpose of Jakobsson's "blinding" operations is to compare blinded results</u>, as opposed to obtaining the same results by performing a falsified operation f(Z) on falsified data as would have been achieved by performing an original operation f on original data, which has the effect of making it impossible to recreate the original operation f. As a result, following Jakobsson's "re-encryption" operation, *i.e.*, the modulo or data combining operations, the results of the data combining operations from different processors are compared, and the process terminates *without compensation for the re-encryption operation*.

Basically, the process of Jakobsson operates as follows:

- a processor of a first "blinding" section, such as processor 20 shown in Fig. 5, first permutes the input (changes the order) and then "re-encrypts" the data (combines it with other numbers, which may be random).
- The results are immediately compared or another "blinding" section is applied and the results are used to "prove" partial correctness of the output (see col. 7, lines 29-47).
- If correct, the permutated results are output. If not, one of the processors or sets of processors is eliminated as un-trustworthy and permutation of the election results continued.

This process does not refer to an auxiliary function value that was *previously* determined by execution of the one or more operations with the auxiliary data as input data in *safe surroundings* and stored along with the auxiliary data. <u>**To the contrary, since the data to combined by Jakobsson with the input data is random, Jakobsson cannot pre-store the auxiliary data in safe surroundings, as claimed**</u>. It is only necessary in Jakobsson that each of the processors to be compared perform predetermined functions. The data or values to be combined do not need to be predetermined.

In the process of Jakobsson, *any* combination of modulo and other operations will work, so long as the results are comparable. The results do not matter, so long as they are the same for each processor or set of processors. If the results are different, then one of the processors or sets of processors is not to be trusted. This is completely contrary to the claimed invention, in which the result of applying function f to the falsified input data (Z combined with input data) must be the same as the result of applying the original function f to the original input data. Accordingly, withdrawal of the rejection of claims 26-33 and 42 in view of the Jakobsson patent is requested.

In addition, since the Jakobsson patent and the remaining references of record also fail to teach the operation disguising operations of, for example, claims 1-21, which should have been examined with the elected claims, allowance of these claims is also respectfully requested.

Having thus overcome each of the rejections made in the Official Action, withdrawal of the rejections and expedited passage of the application to issue is requested.

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
Registration No. 33,805

Date: October 10, 2006

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314
Telephone: (703) 683-0500